UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	Case No. CR19-159-RSL ORDER DENYING MOTION FOR RECONSIDERATION

This matter comes before the Court on defendant Paige Thompson's "Motion to Reconsider Order Denying Defendant's Motion to Dismiss Counts 2 Through 8" (Dkt. # 240). For the reasons explained below, defendant's motion is DENIED.

I. BACKGROUND

On March 21, 2022, the Court issued an Order denying defendant's motion to dismiss Counts 2 through 8 of the second superseding indictment (Dkt. # 226). Counts 2 through 8 allege violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"). See Dkt. # 166. The indictment alleges that defendant created proxy scanners that allowed her to identify Amazon Web Services servers with misconfigured web application firewalls that permitted outside commands to reach and be executed by the servers. Dkt # 166 at ¶ 12. Defendant then allegedly sent commands to the misconfigured servers to obtain security credentials for particular accounts or roles belonging to the victims. Id. at ¶¶ 11-13, 16-18. Defendant allegedly used these "stolen credentials" to "copy data, from folders or buckets of data" in the

victims' cloud storage space and set up cryptocurrency mining operations on the victims' rented servers. Id. at ¶¶ 14-15, 21.

In the Order, the Court considered defendant's argument that she "did not use another person's password or send 'brute force' commands to gain any further access" to the victims' servers, but rather that the system granted her access in response to her commands because it took her for an "authorized visitor." Dkt. # 226 at 6 (quoting Dkt. # 160 at 9). The Court concluded that the indictment clearly alleged that she "accessed the data by using 'stolen credentials' belonging to 'accounts and roles of those customers who had permission to view and copy data.'" Id. (quoting Dkt. # 166 at ¶ 11). The Court advised defendant that her arguments were appropriately made to the trier of fact. Id.

The Court also considered defendant's argument that "because the victims' firewalls were misconfigured, 'anyone with a proxy scanner' could have identified and entered the victim servers, and thus defendant should be 'no more liable under the CFAA than a person accessing a public-facing web page.'" Dkt. # 226 at 7 (citing Dkt. # 123 at 6). The Court observed that this was defendant's "most compelling argument," but nonetheless concluded that it was inconsequential at the motion to dismiss stage because "this argument is properly made to the trier of fact." Id. at 7, 8.

Before reaching this conclusion, the Court remarked that many courts have declined to find a CFAA violation where the information that the defendant accessed is public facing, but that this was not true across the board. Id. at 7. As an example, the Court noted that while the Ninth Circuit concluded in hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) ("hiQ I"), that it was "likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA," Dkt. # 226 at 7-8 (quoting hiQ I, 938 F.3d at 1003), the Supreme Court vacated and remanded this decision for further consideration in light of Van Buren v. United States, 141 S.Ct. 1648 (2021), id. (citing LinkedIn Corp. v. hiQ Labs, Inc., 141 S. Ct. 2752 (2021) (mem.)). The result of this remand remained pending when the Court issued the Order.

On April 18, 2022, the Ninth Circuit issued its opinion on remand in hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022) ("hiQ II"). Defendant now requests that the Court reconsider its original decision in light of hiQ II.

II. DISCUSSION

"Motions for reconsideration are disfavored." Local Rules W.D. Wash. CrR 12(b)(13)(A). Ordinarily, the Court will deny such motions in the absence of a showing of (i) "manifest error in the prior ruling," or (ii) "new facts or legal authority which could not have been brought to its attention earlier with reasonable diligence." Id. Defendant's motion for reconsideration is based on the new legal authority presented in hiQ II. As the Ninth Circuit did not issue hiQ II until a month after the Court issued the Order, hiQ II could not have been brought to the Court's attention earlier with reasonable diligence.

The Court considers defendant's hiQ II-based arguments regarding (A) open accessibility of the servers and (B) the rule of lenity.

A. Open Accessibility

Defendant argues that the Court should reconsider its ruling and dismiss Counts 2 through 8 because under hiQ II, "there can be no viable CFAA charge in the absence of a 'password-protected' server or a server 'that otherwise prevent[s] the general public from viewing [its] information.'" Dkt. # 240 at 4 (quoting hiQ II, 31 F.4th at 1197).[1] In hiQ II, the

[1] Defendant states, "As the Court noted in its order, lack of authorization is a key element as to *all* of the CFAA violations with which Ms. Thompson is charged." Dkt. # 240 at 4 (citing Dkt. # 226 at 3). While this is technically true, defendant implies that lack of authorization *to access* a computer is the key element and that the Court has endorsed this interpretation. This is incorrect. As the Court explained in the original Order:

> Counts 2 through 7 are charged under CFAA subsection (a)(2), which requires "intentionally access[ing] a computer without authorization." 18 U.S.C. § 1030(a)(2). In contrast, Count 8 is charged under CFAA subsection (a)(5)(A), which requires "intentionally caus[ing] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). The Court is cognizant of the need for congruence among these subsections. See [United States v. Nosal, 844 F.3d 1024, 1033 (9th Cir. 2016)]. However, to the extent that defendant's arguments are focused on whether she allegedly *accessed a computer* without

Ninth Circuit explained that "the CFAA contemplates the existence of three kinds of computer systems: (1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given." hiQ II, 31 F.4th at 1197-98. The Ninth Circuit endorsed "the idea that authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information," id., and surmised that "the CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer," id. at 1201. Defendant's argument that hiQ II mandates the Court to dismiss Counts 2 through 8 fails for three reasons.

First, defendant overstates the Court's reliance on hiQ I. Defendant argues that "the Court declined to rule in Ms. Thompson's favor, at least in part" because the Supreme Court had vacated and remanded hiQ I in light of Van Buren. Dkt. # 240 at 4 (citing Dkt. # 260 at 7-8). Defendant is incorrect. The Court reached its ruling because the question of whether the information was public is properly resolved by the trier of fact and is therefore incapable of determination before trial. See United States v. Kelly, 874 F.3d 1037, 1046-47 (9th Cir. 2017) (stating that a motion to dismiss is "capable of determination before trial if it involves questions of law rather than fact" and therefore does not intrude upon "the province of the ultimate finder of fact").

Second, hiQ II does not convert this question of fact to a matter of law. The hiQ II court made it clear that it was only considering LinkedIn profiles "made visible to the general public."

---

authorization, the Court notes that these arguments are not applicable to Count 8, which requires different elements than Counts 2-7.

Dkt. # 226 at 3 n.3. The Court reiterates that defendant's arguments regarding *accessing* a computer without authorization are largely inapplicable to the question of *damaging* a computer without authorization. Defendant's motion therefore again fails to explain why Count 8 should be dismissed.

hiQ II, 31 F.4th at 1185. The LinkedIn information in question was "publicly available data from people who choose to share their information with the world," and "available to anyone with a web browser." Id. at 1189, 1199. The dispute was whether the CFAA prohibited hiQ from scraping this undoubtedly public profile information despite LinkedIn's attempts to thwart such scraping, including anti-scraping tech and delivery of a cease-and-desist letter to hiQ. Id. at 1186-87. The Ninth Circuit observed that "a defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser . . . Van Buren therefore reinforces our conclusion that the concept of 'without authorization' does not apply to public websites." Id. at 1199. Keeping with this, the court explained that a "selective denial of access" is more appropriately characterized as a "ban" than as a "lack of 'authorization.'" Id. at 1196.

The servers at issue in this case occupy a much murkier space than public LinkedIn profiles. The indictment alleges that in order to access the information on these servers, defendant employed a technological process that went beyond merely typing a URL into a browser, or a name into Google, as one would to access a public LinkedIn profile. While proxy scanners may be *available* to the general public, see Dkt. # 240 at 7, it is unclear that this is a technology that the general public actually uses.[2] Lock pick sets are also available to the general public and are typically legal to possess, but a house is not open to the general public simply because a skilled locksmith can successfully pick the lock. Cf. hiQ II, 31 F.4th at 1196 (explaining that the CFAA's legislative history describes CFAA-prohibited conduct as analogous to "breaking and entering"). There is therefore an unresolved question of fact regarding whether these servers were open to the "general public."

Third, the Ninth Circuit did not hold that the servers must be *password*-protected, per se. Rather, the Ninth Circuit explained that "the CFAA's prohibition on accessing a computer

[2] The defense's statement that it has "suggested to the government that this case be tried to the Court because the case involves complex and sensitive issues," Dkt. # 241 at 2, indicates that the defense is aware that the technology in question here extends beyond that which the general public utilizes.

'without authorization' is violated when a person circumvents a computer's *generally applicable rules regarding access permissions*, such as username and password requirements, to gain access to a computer." hiQ II, 31 F.4th at 1201 (emphasis added); see also id. at 1197 ("The legislative history of [the CFAA] thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort."). The indictment alleges that defendant utilized "stolen credentials" to gain access to the servers. Dkt. # 166 at ¶ 11. This sufficiently alleges that defendant circumvented generally applicable rules regarding access permissions. Much of defendant's motion is spent explaining why defendant's conduct did not factually amount to circumventing access permissions and why "stolen credentials" is a misnomer. See Dkt. # 240 at 7-11. Defense counsel forgets that the Court accepts the allegations in the indictment as true and is "bound by the four corners of the indictment" when evaluating a motion to dismiss. United States v. Boren, 278 F.3d 911, 914 (9th Cir. 2002). These arguments are inappropriate at this stage and should be saved for the trier of fact.

B. Rule of Lenity

Finally, defendant argues that the Court should reconsider its ruling "based on the Ninth Circuit's determination in hiQ [II] that rule of lenity requires the CFAA's 'without authorization' provision to be interpreted 'narrow[ly] . . . so as not to turn a criminal hacking statute into a 'sweeping Internet-policing mandate.'" Dkt. # 240 at 11 (quoting hiQ II, 31 F.4th at 1200-01). There are two flaws with this argument.

First, hiQ II's citation to the rule of lenity was in support of its own narrow interpretation of the CFAA's prohibition on access-without-authorization. See hiQ II, 31 F.4th at 1200-01. As explained above, the indictment fulfills hiQ II's narrow interpretation of this provision. The rule of lenity does not now require the Court to narrow the CFAA even more. Cf. Leocal v. Ashcroft, 543 U.S. 1, 12 n.8 (2004) (applying the rule of lenity to interpretation of a criminal statute in a noncriminal context because "we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context").

Second, to the extent that defendant argues that under hiQ II the rule of lenity must be applied "[i]n the absence of the circumvention of a password-protected or otherwise restricted system," Dkt. # 240 at 12, the indictment alleges that defendant accessed the system through the use of "stolen credentials." The indictment must be "construed according to common sense, and interpreted to include facts which are necessarily implied." See United States v. Berger, 473 F.3d 1080, 1103 (9th Cir. 2007) (internal quotation marks and citation omitted). The reference to "stolen credentials" implies that the system was, in some fashion, restricted. The Court reiterates that arguments to the contrary are appropriately made to the trier of fact.

III. CONCLUSION

For the foregoing reasons, IT IS HEREBY ORDERED that defendant's motion for reconsideration (Dkt. # 240) is DENIED.

DATED this 27th day of May, 2022.

Robert S. Lasnik
United States District Judge